REMARKS

I. Status of Prosecution

The above-referenced patent application (the "Patent Application") originally had been filed on October 30, 2003 with twenty (20) claims, three (3) of which were independent in nature. The Patent Application claimed priority to U.S. Provisional Patent Application No. 60/422,720 filed October 31, 2002. A Non-Final Office Action was mailed April 10, 2007. In the Non-Final Office Action, each of claims 1 through 6 were rejected under 35 U.S.C. § 102 (e) as being anticipated by U.S. Patent Publication No. 2003/0188194 by Currie et al. (Currie). Claims 7 through 20, additionally were rejected under 35 U.S.C. § 103(a) as being unpatentable over Currie in view of U.S. Patent Application Publication No. 2002/0178383 by Hrabik et al. (Hrabik). Most recently, the Examiner agreed to a personal interview in order to discuss a resolution to the present rejections. The Applicants are most appreciative of the Examiner's conduct of such interview.

II. Invention Summary

The Applicant has invented a system and method for intrusion detection. In accordance with the Applicant's invention, an intrusion detection system monitors the rate and characteristics of Internet attacks on a computer network and filters attack alerts based upon various rates and frequencies of the attacks. Notably, the intrusion detection system monitors attacks on other hosts and determines if the attacks are random or general attacks or attacks directed towards a specific computer network and generates a corresponding signal. The intrusion detections system also tests a computer network's vulnerability to attacks detected on the other monitored hosts.

III. Re-statement of Examiner Argument

In the Non-Final Office Action, the Examiner contended that Currie taught generally the notion of intrusion detection and providing alerts based upon detecting multiple attacks. The Examiner also contended that the combination of Currie and Hrabik taught intrusion detection with respect to multiple networks.

IV. Claim Amendments

In the Applicant's invention, attacks on multiple different external networks can be monitored, such as attacks on multiple sources, multiple targets and/or multiple ports. An example would include detecting "self-propagating worms" as described in page 19 lines 1 through 5 of the Patent Application. Using the information gleaned from monitoring the attacks on the external networks, an attack upon a completely different network can be characterized as a "general attack" or a "client specific attack". Consequently, attacks of a higher priority (client specific attacks) can be handled with a higher priority than attacks of a lower priority (general attack).

Based upon the distinctive nature of the Applicant's invention described herein, the Applicant believes that amended claims 1, 12 and 16 highlight the observation of attacks on a plurality of external networks in order to characterize an attack on a separate network as one of a client specific attack or a general attack.

V. Conclusion

The Applicants appreciate the Examiner's conduct of the Personal Interview and Applicants respectfully request the withdrawal of the rejections under 35 U.S.C. §§ 102(e) and 103(a) owing to the amended claims and the foregoing remarks. The

Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: June 3, 2007

/Steven M. Greenberg/

Steven M. Greenberg, Reg. No.: 44,725
Attorney for Applicant(s)
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle
Suite 3020
Boca Raton, Florida 33487
Customer No. 29973
Tel: (561) 922-3845
Fax: (561) 244-1062